Case Study

DSW21 Dortmunder Stadtwerke AG

Vorgehen und Erfahrungen bei der Implementierung und Umsetzung eines integrierten Datenschutz- und Informationssicherheitsmanagementsystems mit QSEC

Dr. Paul-Martin Steffen, Leitung Datenschutz und Informationssicherheit bei DSW21 Dortmunder Stadtwerke AG, berichtet über die Vorgehensweise und die Erfahrungen bei der Implementierung und Umsetzung eines integrierten Datenschutz- und Informationssicherheitsmanagementsystems mit QSEC.

Das Unternehmen

DSW21 bietet seit 1857 Leistungen der Daseinsvorsorge für alle Dortmunder*innen an. Die Daseinsvorsorge ist das Kerngeschäft der 21-Familie. Zum Konzern gehören Tochterfirmen, Beteiligungen und Anteile an weiteren Unternehmen. Sie alle kümmern sich um die Infrastruktur und Dienstleistungen des täglichen Lebens.

Der Konzern gliedert sich in die vier Bereiche:

Mobilität + Logistik:

Zur Sparte Mobilität und Logistik gehören unter anderem der Nahverkehr mit 120 Stadtbahn-Wagen, mehr als 200 Bussen und über 100 Millionen Fahrgästen pro Jahr, die H-Bahn 21, der Dortmunder Hafen 21 und der Dortmund Airport 21 mit mehr als 2,6 Millionen Fluggästen (2022).

Lebensräume:

Städte verändern sich. In Dortmund sind viele ehemalige Industrie- und Militärflächen für neue Nutzungen freigeworden. Das beeindruckendste Beispiel ist der Phoenix-See. Wo bis Anfang der 2000-er Jahre eines der größten Stahlwerke des Ruhrgebiets stand, lädt heute ein Freizeitsee nun zum Bummeln an der Hafenpromenade ein. Umgeben von Büro- und Wohnhäusern ist der Phoenix-See ein Projekt mit internationaler Strahlkraft. Aber auch zwei ehemaligen Arealen der britischen Rheinarmee hat der Konzern 21 zu einem völlig neuen Gesicht verholfen: der Stadtkrone-Ost (Gewerbe, Technologie & Wohnen) sowie Hohenbuschei (Wohnen & BVB-Leistungszentrum).

Energie + Wasser:

DEW21 ist das Unternehmen für Strom, Wärme, Wasser. Aber auch eigene Energieerzeugung sowie komplexe umweltschonende Gesamtlösungen sind Teil der vielfältigen Aufgaben des lokal-regionalen Energieversorgers. DEW21 wurde 1995 gegründet. Das Unternehmen überzeugt als Dienstleister vor Ort, aber auch als deutschlandweiter Anbieter.

Datennetze:

Sichere Netze für Internet, Telefonie und Datenaustausch bietet DOKOM21. Dazu ist der regional geprägte Kommunikationsdienstleister der 21-Familie der größte Betreiber von Rechenzentren im Ruhrgebiet und Partner der Digitalen Stadt Dortmund mit WLAN-Angeboten und anderen digitalen Mehrwerten und Produkten. DOKOM21 stemmt zudem einen Teil des Breitbandausbaus in Dortmund und versorgt die Bürger*innen über Glasfaseranschlüsse mit schnellem Internet

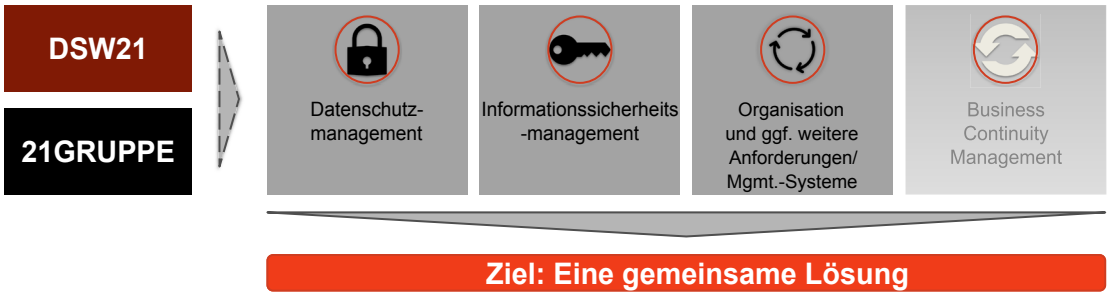


Abbildung folgender Zielsetzung

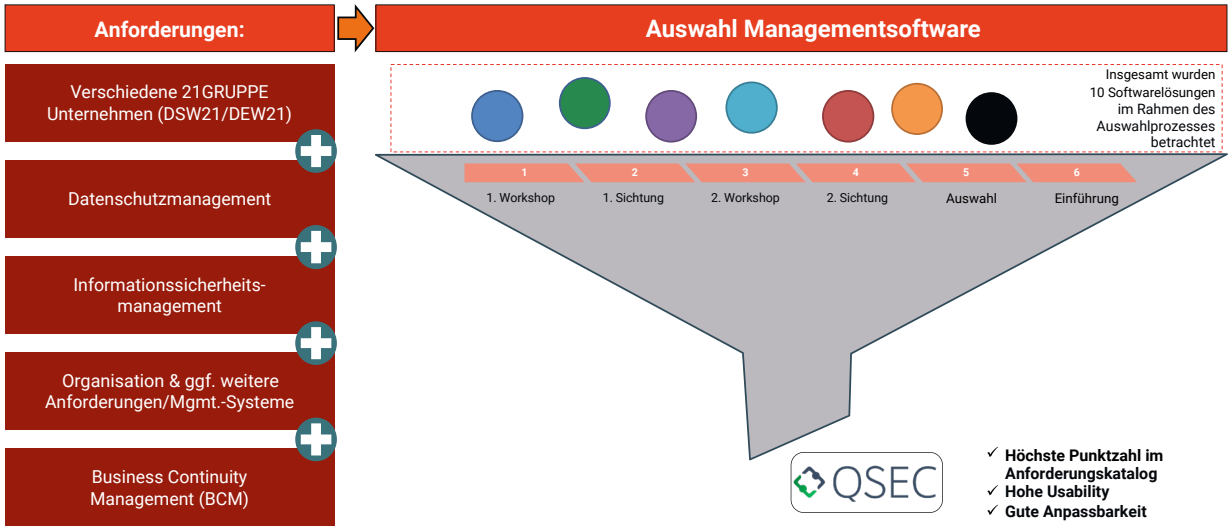
- Abdeckung der regulatorischen Anforderungen
- Sicherstellung einer prüfgerechten Dokumentation (Revisionsicherheit)
- Ganzheitliche Abbildung der Managementsysteme sowie deren Softwarebasierte Unterstützung

Die Ausgangssituation und Zielsetzung

Die Ausgangssituation bei DSW21 vor dem Start der Toolauswahl für die Implementierung eines integrierten Datenschutz- und Informationssicherheitsmanagementsystems kann in den betroffenen Bereichen Informationssicherheit, Datenschutz, Qualitätsmanagement und Organisation als sehr unterschiedlich bezeichnet werden. In den verschiedenen Bereichen wurden vor der Einführung von QSEC die Anforderungen in Bezug auf KRITIS-Anforderungen, Datenschutzmanagement und Qualitätsmanagement im Schwerpunkt unter Nutzung von Word- und Excel-Templates umgesetzt. Im Bereich der Organisation wurden Organigramme in Visio gepflegt und Prozesse primär in Verfahrensrichtlinien und Funktionsbeschreibungen hinterlegt.

Die Zielsetzung war, eine Softwarelösung zu etablieren, mit der einerseits alle Anforderungen an das Datenschutz- und Informationssicherheitsmanagement abgedeckt werden können und andererseits die Option bestehen sollte, auch die Organisation und ggf. weitere Managementsystem bis hin zum Business Continuity Management abbilden zu können.

Wesentliche Grundanforderungen dafür waren: die Abdeckung der regulatorischen Anforderungen, die Sicherstellung einer prüfgerechten Dokumentation (Revisionssicherheit) und die ganzheitliche softwarebasierte Abbildung der Managementsysteme.



Der Auswahl- und Entscheidungsprozess

Grundlage des Auswahlprozesses der Software war ein detaillierter Anforderungskatalog an eine Softwarelösung, der nachfolgend aufgeführte Kapitel beinhaltete:

- Funktionale Anforderung (übergreifen)
- Nichtfunktionale Anforderungen (übergreifend)
- Schnittstellen (übergreifend)
- Datenschutz
- Informationssicherheit
- Organisation
- Business Continuity Management

Methodik:

Insgesamt wurden im Auswahlprozess 10 Softwarelösungen betrachtet, die in unterschiedlichen Workshops und Terminen gesichtet und bewertet wurden. Bei der finalen Auswahl der zu etablierenden Lösung wurde insbesondere auf einen hohen Erfüllungsgrad des Anforderungskataloges und eine gute Benutzerfreundlichkeit Wert gelegt.

DSW21

QSEC konnte über den gesamten Zyklus des Auswahlprozesses überzeugen und hat letztlich den Zuschlag erhalten. Hervorzuhebende Punkte waren im Bewertungsprozess auch die in QSEC implementierte Methodik, der umfassende in QSEC enthaltene Content und die unterschiedlichen Anwendermodi für Experten und Anwender aus den Fachabteilungen. Dies alles sprach neben den reinen Leistungsdaten für eine Zusammenarbeit mit Nexis GRC und den Einsatz von QSEC.

Die Einführungsphase

Die Implementierung von QSEC und der Rollout wurden in mehrere Phasen untergliedert.

Phase 1

Zunächst wurden in Zusammenarbeit mit Nexis GRC die Grundkonfiguration des Systems umgesetzt und u. a. Werteskalen, Methodiken, Logos, Reports und Geschäftseinheiten eingerichtet. In dieser Phase wurden auch bereits unternehmensspezifische Vorgaben in QSEC umgesetzt.

Phase 2

In Phase 2 wurde die Inbetriebnahme beim IT-Dienstleister vorbereitet. Das System wurde durch Nexis GRC installiert, die Zugänge und die AD-Anbindung eingerichtet und die Schulungsmaterialien für Führungskräfte und Mitarbeitende vorbereitet. In dieser Phase wurde auch ein internes Handbuch zur Festlegung einheitlicher Namenskonventionen und Hinweise zur Pflege der Daten umgesetzt.

Phase 3

Die Basis-Befüllung für DSW21 erfolgte in Phase 3. Hierzu gehörte u.a. die Aufbereitung der bestehenden Informationen zu Prozessen, Informationen, Assets und Dienstleistern. Die Übertragung und der Import der aufbereiteten Daten, weitere Detailkonfiguration des Systems und die Anpassung von Einstellungen sowie die Festlegung der Nomenklatur (z. B. für interne IDs, Assets). Im Ergebnis waren in QSEC die Geschäftsprozesse, die zugehörigen Informationen, die Assetgruppen und die Dienstleistenden befüllt.

Phase 4

In Phase 4 (ongoing) erfolgt/erfolgte der Rollout bei DSW21. Wichtige Aspekte hierbei sind/waren die Durchführung von Auftaktgesprächen mit den Fachbereichen zur Darstellung der Vorgehensweise, die Vorstellung des „Interview Wizards“ und die gemeinsame Pflege eines Prozesses. Ab dieser Phase erfolgt/erfolgte auch die eigenverantwortliche weitere Pflege des Systems durch die Koordinierenden in den Fachbereichen und die Übernahme der aktualisierten Prozesse wurde vom Datenschutzbeauftragten und Informationssicherheitsbeauftragten mittels des „Interview Übernahme Wizards“ geprüft.

Phase 5

In der Phase 5 (ongoing) wird/wurde der Rollout in die 21GRUPPE umgesetzt. Wichtige Aspekte hierbei ist/war die „Abholung“ der Koordinierenden aus den verschiedenen Gesellschaften, die Übertragung von Basis-/Standardprozessen in die Gesellschaften und die Durchführung der Interviews analog zu DSW21 mit anschließender Übernahme.

Phase 6

In Phase 6 (ongoing) wird/wurde das System in den Regelbetrieb überführt und ein kontinuierlicher Verbesserungsprozess etabliert.

In den Phasen 3-6 wurden parallel auch weitere QSEC-Module (Security Incidents, Maßnahmen und IT-Risiko) in Betrieb genommen.

DSW21

Fazit und Ausblick

Insgesamt blicken wir bei DSW21 und der 21-Gruppe bereits auf ein sehr erfolgreiches Projekt.

Wichtige Erkenntnisse sind/waren

» die Notwendigkeit, einheitliche Strukturen und Grundlagen für die Überführung der benötigten Informationen in QSEC zu schaffen und

» die Erfordernis, Fachbereiche bei der Nutzung der Software zu begleiten.

Positive Erfahrungen sind

» die Schaffung einer einheitlichen, validen Datenbasis,

» die Abbildung und Nachvollziehbarkeit von Zusammenhängen sowie

» die Etablierung einer revisionssicheren Dokumentation.

In naher Zukunft ist die

» verstärkte Nutzung des Reporting-Moduls für aussagefähige Berichte,

» die Nutzung von QSEC im Rahmen kommender Audits und

» die Nutzung des Business Continuity Moduls geplant.

„Wir sind mit der Leistungsfähigkeit von QSEC zusammenfassend betrachtet sehr zufrieden und werden die Software zukünftig weiter ausprägen und intensiv nutzen. Der Hersteller der Software, Nexis GRC, ist dabei für uns ein verlässlicher Partner, der uns mit jahrzehntelanger Erfahrung aus der Umsetzung weltweiter GRC und ISMS-Projekte stets bestmöglich unterstützt.“

Dr. Paul-Martin Steffen: Leitung Datenschutz und Informationssicherheit, DSW21 Dortmunder Stadtwerke AG

In Zusammenarbeit von Nexis GRC und DSW21

Besuchen Sie unsere Webinare zu den verschiedensten Themen auf:
www.nexis-qsec.com

Sie können auch direkt eine Web-Demo mit uns vereinbaren und Einblick in QSEC erlangen unter:
www.nexis-qsec.com

Für weitere Fragen stehen wir Ihnen jederzeit zur Verfügung:
Nexis GRC GmbH • Zimmerstraße 1, 22085 Hamburg • +49 40 650336-0 • info@nexis-qsec.com